Information Commissioner's Office

Consultation:

Age Appropriate Design code

Start date:15 April 2019

End date: 31 May 2019

ico.
Information Commissioner's Office

Introduction

The Information Commissioner is seeking feedback on her draft code of practice Age appropriate design - a code of practice for online services likely to be accessed by children (the code).

The code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet.

The code is now out for public consultation and will remain open until 31 May 2019. The Information Commissioner welcomes feedback on the specific questions set out below.

Please send us your comments by 31 May 2019.

Download this document and email to:
ageappropriatedesign@ico.org.uk

Print off this document and post to:
Age Appropriate Design code consultation
Policy Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to the Policy Engagement Department about the Age Appropriate Design code or email ageappropriatedesign@ico.org.uk

Privacy statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public or a parent). All responses from organisations and individuals responding in a professional capacity (e.g. academics, child development experts, sole traders, child minders, education professionals) will be published. We will remove email addresses and telephone numbers from these responses but apart from this, we will publish them in full.

For more information about what we do with personal data, please see our privacy notice.

Section 1: Your views

Q1. Is the '**About this code'** section of the code clearly communicated?

Yes

Q2. Is the '**Services covered by this code'** section of the code clearly communicated?

YES/NO.

CCO strongly supports the breadth of the provision in section 123 of the DPA in applying not only to services aimed at children, but also those likely to be used by children. DCMS should adopt the same approach in the development of their online harms legislation to ensure that the two frameworks complement one another.

The key principle that the code applies to services likely to be accessed by children, whether or not this was intended by the developers, is well communicated in the draft code. However this section requires the addition of thresholds. For example, the code states that if evidence emerges that a "significant number" of children are accessing a service, the service will need to be made compliant with the code – there needs to be an indication of what constitutes a "significant number".

There must also be a mechanism in place to ensure that providers are gathering the necessary evidence to determine the number of children using their services. CCO would support the introduction of a requirement on providers to comply with information requests from the ICO.

Standards of age-appropriate design

Please provide your views on the sections of the code covering each of the 16 draft standards

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

2. Age-appropriate application: Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

3. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

4. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

5. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

6. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

7. Data minimisation: Collect and retain only the minimum amount of personal data necessary to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

9. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

10. Parental controls: If you provide parental controls give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

11. Profiling: Switch options based on profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

12. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off privacy protections, or extend use.

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this code

14. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

15. Data protection impact assessments: Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

16. Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code

Q3. Have we communicated our expectations for this standard clearly?

1. **Best interests of the child**
Yes CCO welcomes the emphasis on the best interests of the child in the first provision of the code. It provides a clear statement of purpose for the code and sets out to providers what their most important consideration must always be. The code helpfully points to Article 5 and Recital 38 of the GDPR, demonstrating the requirements that ISS providers must already meet under existing legislation.
2. Age-appropriate application
YES/NO. CCO strongly supports the requirement that the code must be applied to all users unless a robust form of age verification is in place. We agree that the current practice of asking users to submit their own age must be ended, as it is too easy for children to simply lie about their age. Expectations for what constitutes a "robust" form of age verification must be very high – this is not unreasonable given technology currently available to ISS providers and the rapid pace of innovation in this field. CCO has been assured that it is possible. This section is mostly clear but would benefit from a few points of refinement:

Many children begin using certain platforms on their parent's device (e.g. phone or tablet), before they are given their own. This raises an additional challenge for age verification that providers must address if their methods are to be considered robust.

CCO welcomes the inclusion of a 0-5 age bracket in the code in recognition of the fact that many children now have their data processed in their earliest years. It could be made clearer that the provisions of the code apply even if the processing of the child's data is entirely mediated by the parent, as can be the case with internet-enabled devices (e.g. connected baby cameras).

The inclusion of the 10-12 age bracket is also welcome. As made clear in our Life in Likes research, children's use of digital services changes significantly during this period, becoming less about playing games and connecting with family members and more about cementing friendships and keeping up with trends. This introduces new pressures. The particular importance of the transition years should be flagged in this section of the code.

3. Transparency

YES/NO

The code helpfully elaborates the ways in which providers can present terms and conditions in child-friendly ways, including through video and audio content, pop ups and and cartoons. The ICO should request data from providers on how far children engage with these methods, to ensure that providers are always seeking to improve the ways they deliver information to children.

This section states that providers must adapt their methods to services that are not screen based (e.g. connected toys), but lots of the language and ideas used in this section are screen-centric. The section would therefore benefit from an example of good practice for a non-screen based service.

4. Detrimental use of data

Yes

CCO supports the statement of the provisions in this section, including the emphasis on a precautionary principle.

5. Policies and community standards

Yes

CCO supports the statement of the provisions in this section.

6. Default settings

YES/NO.

CCO welcomes the principle of privacy by default, in light of the fact that most users will not change their default privacy settings.

Further clarification in this section would help. The code is correct to set out that there may sometimes be a compelling reason for a privacy function not to be turned off by default, but it should make it clearer that the expectation is for those occasions to be rare. What constitutes a "compelling reason" should be explained in greater depth.

The summary of the provision should read "…taking account of the best interests of the child as a primary consideration" - "As a primary consideration" is a crucial addition to clarify that above all it is the best interests of the child that come first, as made clear in the first standard.

Finally, the point should be made that some settings will never be appropriate for children, and turning them off by default is not a good enough solution.

7. Data minimisation

Yes

CCO supports the statement of the provisions in this section.

8. Data sharing

YES/NO.

Similar to the 6th standard, CCO would like to see the summary of this refer to the best interests of the child as a primary consideration:
"Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child as a primary consideration". "Compelling reason" must also be explained in greater depth so that it is clear what will meet this bar in practice.

As discussed in our report 'Who Knows What About Me?', CCO believes it is crucially important that children and parents are made aware of when their data is being shared and with who. Although it is stated in this section that GDPR requires providers to inform subjects when their data is shared, more should be said about the expectations on them to do this in an age appropriate way.

9. Geolocation

YES/NO.

CCO strongly supports geolocation being turned off by default for children. The statement of standard could be slightly clearer: again CCO

would like "as a primary consideration" included in the summary of this provision and for "compelling reason" to be explained in more depth.

10. Parental controls

Yes

CCO supports the statement of the provisions in this section.

11. Profiling

No

CCO believes the provisions in this section could be stronger.

As with previous provisions, "compelling reason" needs to be detailed in full and the best interests of the child should be taken into account "as a primary consideration".

Crucially, the provision needs to be clearer about the fact that profiling of children should not be the norm, as set out in Recital 71 to the GDPR. This demands more than profiling being switched off by default and for appropriate measures to be in place to protect the child from harmful effects, as currently proposed. There should be a demonstrable reason why any profiling is necessary at all – i.e. that it is in the child's best interests and that it is crucial to the specific service being delivered. It is correct that it is difficult for children to understand how their personal data is being used in profiling and what the consequences of that might be, simply because the consequences at this stage are unknown – as set out in CCO's report 'Who Knows What About Me?'. For this reason a precautionary approach is necessary and profiling of children should be extremely limited.

12. Nudge techniques

Yes

CCO welcomes the inclusion of this provision. Although there is growing awareness of the influence of nudge techniques, e.g. in preventing children from switching off from social media and the impact of that on their mental health, there has been less discussion of the impact on their privacy. This section makes clear that nudge techniques which lead children to make poor privacy decisions will no longer be tolerated.

CCO is particularly concerned about the use of addictive and immersive desgin features in online games. Children tell us that they can feel compelled to behave in a certain way, such as to gamble (either in-game currency or real money), in order to access certain features of the game, as the game is so addictive. CCO will be publishing a report about

children's experiences of online gaming later this year. Given the possible risks, it would be beneficial for this section (and indeed the entire code) to include more examples related to gaming.
13. Connected toys and devices
Yes CCO strongly supports the inclusion of a specific standard on connected toys and devices. The privacy risks associated with these products were discussed in our recent report 'Who Knows What About Me?'. The Government has since put forward its new IoT proposals and it will be crucial that the code is updated so that they complement one another - for example using the same definition of a connected toy/device. Developers of connected products face particular challenges in complying with the code, as noted in the provision. The products are often not screen-centric and devices might be used by very young children (sometimes babies, in the case of connected baby cameras). Nevertheless it is crucial that the same high expectations are adopted for providers of these services.
14. Online tools
Yes CCO supports the statement of the provisions in this section.
15. Data protection impact assessments
Yes CCO supports the statement of the provisions in this section.
16. Governance and accountability
Yes CCO supports the statement of the provisions in this section.

Q4. Do you have any examples that you think could be used to illustrate the approach we are advocating for this standard?

1. **Best interests of the child**
Yes Lego Life is an example of a social media platform which aims to protect the best interests of the child through its design. All content uploaded to the platform is pre-moderated and children chat through emojis, allowing

children to express themselves in a playful, creative way while also staying safe. CCO has also previewed the BBC's new Own It app, which was announced at the end of last year. The app will combine machine-learning technology with kids self-reporting their own online activity and moods. In response, the app will provide advice and support when the child needs it.
2. Age-appropriate application
YES/NO. If YES, then please provide details.
3. Transparency
YES/NO. If YES, then please provide details.
4. Detrimental use of data
YES/NO. If YES, then please provide details.
5. Policies and community standards
YES/NO. If YES, then please provide details.
6. Default settings:
YES/NO. If YES, then please provide details.
7. Data minimisation
YES/NO. If YES, then please provide details.
8. Data sharing
YES/NO. If YES, then please provide details.
9. Geolocation
YES/NO. If YES, then please provide details.
10. Parental controls
YES/NO.

If YES, then please provide details.
11. Profiling
YES/NO. If YES, then please provide details.
12. Nudge techniques
YES/NO. If YES, then please provide details.
13. Connected toys and devices
YES/NO. If YES, then please provide details.
14. Online tools
YES/NO. If YES, then please provide details.
15. Data protection impact assessments
YES/NO. If YES, then please provide details.
16. Governance and accountability
YES/NO. If YES, then please provide details.

Q5. Do you think this standard gives rise to any unwarranted or unintended consequences?

1. **Best interests of the child**
No CCO recognises that a tension can exist between allowing children to participate online and protecting them from harm. However existing good practice shows that the two do not necessarily need to be in conflict - if providers think creatively while also adopting a Privacy by Design approach they can continue to provide exciting products that enhance children's lives.
2. Age-appropriate application

YES/NO. If YES, then please provide your reasons for this view.
3. Transparency
YES/NO. If YES, then please provide your reasons for this view.
4. Detrimental use of data
YES/NO. If YES, then please provide your reasons for this view.
5. Policies and community standards
YES/NO. If YES, then please provide your reasons for this view.
6. Default settings
YES/NO. If YES, then please provide your reasons for this view.
7. Data minimisation
YES/NO. If YES, then please provide your reasons for this view.
8. Data sharing
YES/NO. If YES, then please provide your reasons for this view.
9. Geolocation
YES/NO. If YES, then please provide your reasons for this view.
10. Parental controls
YES/NO. If YES, then please provide your reasons for this view.
11. Profiling
YES/NO. If YES, then please provide your reasons for this view.
12. Nudge techniques
YES/NO. If YES, then please provide your reasons for this view.
13. Connected toys and devices
YES/NO. If YES, then please provide your reasons for this view.
14. Online tools

YES/NO. If YES, then please provide your reasons for this view.
15. Data protection impact assessments
YES/NO. If YES, then please provide your reasons for this view.
16. Governance and accountability
YES/NO. If YES, then please provide your reasons for this view.

Q6. Do you envisage any feasibility challenges to online services delivering this standard?

1. **Best interests of the child**
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
2. Age-appropriate application
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
3. Transparency
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
4. Detrimental use of data
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
5. Policies and community standards
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
6. Default settings
YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
7. Data minimisation
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
8. Data sharing
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
9. Geolocation
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
10. Parental controls
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
11. Profiling
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
12. Nudge techniques
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
13. Connected toys and devices
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
14. Online tools
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
15. Data protection impact assessments
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

16. Governance and accountability
YES/NO. If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

Q7. Do you think this standard requires a transition period of any longer than 3 months after the code come into force?

1. **Best interests of the child**
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
2. Age-appropriate application
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
3. Transparency
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
4. Detrimental use of data
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
5. Policies and community standards
No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
6. Default settings
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
7. Data minimisation
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
8. Data sharing
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
9. Geolocation
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
10. Parental controls
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
11. Profiling
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
12. Nudge techniques
No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
13. Connected toys and devices
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
14. Online tools
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
15. Data protection impact assessments
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
16. Governance and accountability
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Q8. Do you know of any online resources that you think could be usefully linked to from this section of the code?

1. **Best interests of the child**
YES/NO. If YES, then please provide details (including links).
2. Age-appropriate application
YES/NO. If YES, then please provide details (including links).

3. Transparency
YES/NO. If YES, then please provide details (including links).
4. Detrimental use of data
YES/NO. If YES, then please provide details (including links).
5. Policies and community standards
YES/NO. If YES, then please provide details (including links).
6. Default settings
YES/NO. If YES, then please provide details (including links).
7. Data minimisation
YES/NO. If YES, then please provide details (including links).
8. Data sharing
YES/NO. If YES, then please provide details (including links).
9. Geolocation
YES/NO. If YES, then please provide details (including links).
10. Parental controls
YES/NO. If YES, then please provide details (including links).
11. Profiling
YES/NO. If YES, then please provide details (including links).
12. Nudge techniques
Yes If YES, then please provide details (including links).
13. Connected toys and devices
No If YES, then please provide details (including links).
14. Online tools
YES/NO. If YES, then please provide details (including links).

15. Data protection impact assessments
YES/NO. If YES, then please provide details (including links).
16. Governance and accountability
YES/NO. If YES, then please provide details (including links).

Q9. Is the '**Enforcement of this code'** section clearly communicated? Yes
Q10. Is the '**Glossary'** section of the code clearly communicated? Yes
Q11. Are there any key terms missing from the '**Glossary'** section? No
Q12. Is the '**Annex A: Age and developmental stages'** section of the code clearly communicated? Yes

Q13. Is there any information you think needs to be changed in the **'Annex A: Age and developmental stages**' section of the code?

No

Q14. Do you know of any online resources that you think could be usefully linked to from **the 'Annex A: Age and developmental stages**' section of the code?

Yes

In addition to our report on children's data, CCO produced an interactive infographic exploring the kids of data collected from children at different ages, which can be seen here: https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/

Q15. Is the **'Annex B: Lawful basis for processing'** section of the code clearly communicated?

Yes

Q16. Is this **'Annex C: Data Protection Impact Assessments'** section of the code clearly communicated?

No

Q17. Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation?

No

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	☒
A body representing the views or interests of parents? Please specify:	☐
A child development expert? Please specify:	☐

An Academic? Please specify:	☐
An individual acting in another professional capacity? Please specify:	☐
A provider of an ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public or a parent)?	☐
An ICO employee?	☐
Other? Please specify:	☐

Thank you for responding to this consultation.

We value your input.